



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/044,019	01/11/2002	Partha Bhattacharya	50325-0629	8175

29989 7590 05/10/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER

MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 05/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/044,019	Applicant(s) BHATTACHARYA ET AL.	
	Examiner Aravind K. Moorthy	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 March 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,6,7,9-11,14-17,25-27 and 29-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,6,7,9-11,14-17,25-27 and 29-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 October 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the RCE filed on 10 March 2006.
2. Claims 1, 6, 7, 9-11, 14-17, 25-27 and 29-32 are pending in the application.
3. Claims 1, 6, 7, 9-11, 14-17, 25-27 and 29-32 have been rejected.
4. Claims 2-5, 8, 12, 13, 18-24 and 28 have been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10 March 2006 has been entered.

Response to Arguments

6. Applicant's arguments with respect to claims 1, 6, 7, 9-11, 14-17, 25-27 and 29-32 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 6, 7, 9-11, 14-17, 25-27 and 29-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Freed et al U.S. Patent No. 7,039,053 B1.

As to claim 1, Freed et al discloses a method of comparing access control lists to configure a security policy on a network, the method comprising the computer-implemented steps of:

identifying first sub-entries in a first access control list [column 5, lines 18-29];

identifying second sub-entries in a second access control list [column 5, lines 60-64];

programmatically determining whether a first access control list is functionally equivalent to a second access control list in order to configure the security policy on the network by determining whether each first sub-entry in the first access control list is equivalent to at least one of the second sub-entries [column 5, lines 38-59]; and

determining that the first access control list is functionally equivalent to the second access control list only when each of the first sub-entries is equivalent to at least one of the second sub-entries [column 6, lines 11-54];

wherein programmatically determining whether the first access control list is equivalent to the second access control list comprises:

identifying a dimensional range for each policy action specified in the first access control list, the dimensional range of each policy action

characterizing communication packets specified by entries in the first access control list for that policy action [column 6, lines 11-54];

identifying a dimensional range for each policy action specified in the second access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the second access control list for that policy action [column 7, lines 35-56]; and

determining whether the dimensional range identified for each policy action in the first access control list is equivalent to the dimensional range identified for each policy action in the second access control list [column 7, lines 35-56];

wherein identifying the dimensional range for each policy action specified in the first access control list and in the second access control list comprises at least one step from a set of steps comprising:

identifying a source Internet Protocol (IP) address range and a destination IP address range for communication packets specified by each of the entries in the first access control list and in the second access control list [column 7, lines 35-56];

identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list and in the second access control list [column 7, lines 35-56]; and

identifying a communication protocol for communication packets specified by each of the entries in the first access control list and in the second access control list [column 7, lines 35-56].

As to claim 6, Freed et al discloses that the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein programmatically determining whether a first access control list is equivalent to the second access control list includes:

determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the second access control list that specify the policy action of the entry in the first access control list [column 8, lines 12-46].

As to claim 7, Freed et al discloses that the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein programmatically determining whether a first access control list is equivalent to the second access control list includes:

determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the second access control list that specify the policy action of the entry in the first access control list [column 8, lines 12-46]; and

determining whether each entry in the second access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the first access control list that specify the same policy action [column 8, lines 12-46].

As to claim 9, Freed et al discloses an apparatus for comparing access control lists to configure a security policy on a network, the apparatus comprising:

a processor [column 3 line 65 to column 4 line 27];

a network interface that communicative couples the processor to the network to receive flows of packets therefrom [column 3 line 65 to column 4 line 27];

a memory [column 3 line 65 to column 4 line 27]; and

sequences of instructions in the memory which, when executed by the processor, cause the processor to carry out steps of:

identifying a dimensional range and a policy action for each entry in a first access control list [column 4, lines 46-60];

identifying all overlapping dimensional ranges in the first access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the first access control list overlap [column 5 line 60 to column 6 line 54];

identifying all non-overlapping dimensional ranges in the first access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the first access control

list that do not overlap dimensional ranges of other entries in the first access control list [column 5 line 60 to column 6 line 54];

identifying a policy action for each identified overlapping dimensional range of the first access control list [column 5 line 60 to column 6 line 54];

identifying a policy action for each identified non-overlapping dimensional range of the first access control list [column 5 line 60 to column 6 line 54]; and

determining whether each identified overlapping and non-overlapping dimensional range identified from the first access control list is contained by or equal to a dimensional range of entries in a second access control list in which the entries of the second access control list have the policy action of that identified overlapping or non-overlapping dimensional range [column 5 line 60 to column 6 line 54];

wherein identifying a policy action for each identified overlapping dimensional range of the first access control list includes using a conflict rule to determine the policy action from a first policy action of a first entry having a dimensional range within the overlapping dimensional range, and from a second policy action of a second entry having a dimensional range within the overlapping dimensional range, wherein the second policy conflicts with the first policy [column 5 line 60 to column 6 line 54];

wherein using the conflict rule to determine the policy action comprises selecting one of the first policy and the second policy based on a selected policy of the first and second policies being newer than an unselected policy of the first and second policies [column 5 line 60 to column 6 line 54].

As to claim 10, Freed et al discloses that the steps further comprise:

identifying a dimensional range and a policy action for each entry in the second access control list [column 6 line 59 to column 7 line 34];

identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap [column 6 line 59 to column 7 line 34];

identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list [column 6 line 59 to column 7 line 34];

identifying a policy action for each identified overlapping dimensional range in the second access control list [column 6 line 59 to column 7 line 34];

identifying a policy action for each identified non-overlapping dimensional range of the second access control list [column 6 line 59 to column 7 line 34]; and

determining whether each identified overlapping and non-overlapping dimensional range identified from the second access control list is contained by or equal to a dimensional range of entries in the first access control list in which the entries of the first access control list have the policy action of that identified overlapping or non-overlapping dimensional range [column 6 line 59 to column 7 line 34].

As to claim 11, Freed et al discloses that the steps further comprise:

identifying a dimensional range and a policy action for each entry in the second access control list [column 6 line 59 to column 7 line 34];

identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap [column 6 line 59 to column 7 line 34];

identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list [column 6 line 59 to column 7 line 34];

identifying a policy action for each identified overlapping dimensional range of the second access control list [column 6 line 59 to column 7 line 34];

identifying a policy action for each identified non-overlapping dimensional range of the second access control list [column 6 line 59 to column 7 line 34]; and

wherein determining whether each identified overlapping and non-overlapping dimensional range of the first access control list is contained by or equal to a dimensional range of entries in a second access control list includes determining whether each identified overlapping and non-overlapping dimensional range identified from the first access control list is contained by or equal to overlapping and non-overlapping dimensional ranges of the second access control list [column 6 line 59 to column 7 line 34].

As to claim 14, Freed et al discloses that identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list [column 4, lines 46-60].

As to claim 15, Freed et al discloses that identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list [column 4, lines 46-60].

As to claim 16, Freed et al discloses that identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a communication protocol for communication packets specified by each of the entries in the first access control list [column 4, lines 46-60].

As to claim 17, Freed et al discloses a computer readable medium for comparing access control lists to configure a security policy on a network, the computer readable medium carrying instructions for performing the steps of:

identifying first sub-entries in a first access control list [column 5, lines 18-29];

identifying second sub-entries in a second access control list [column 5, lines 60-64];

programmatically determining whether a first access control list is functionally equivalent to a second access control list in order to configure the security policy on the network by determining whether each first sub-entry is equivalent to at least one of the second sub-entries [column 5, lines 38-59]; and

determining that the first access control list is functionally equivalent to the second access control list only when each of the first sub-entries is equivalent to at least one of the second sub-entries [column 6, lines 11-54];

wherein programmatically determining whether the first access control list is equivalent to the second access control list comprises:

identifying a dimensional range for each policy action specified in the first access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the first access control list for that policy action [column 6, lines 11-54];

identifying a dimensional range for each policy action specified in the second access control list, the dimensional range of each policy action

characterizing communication packets specified by entries in the second access control list for that policy action [column 7,lines 35-56]; and

determining whether the dimensional range identified for each policy action in the first access control list is equivalent to the dimensional range identified for each policy action in the second access control list;

wherein identifying the dimensional range for each policy action specified in the first access control list and in the second access control list comprises at least one step from a set of steps comprising:

identifying a source Internet Protocol (EP) address range and a destination IP address range for communication packets specified by each of the entries in the first access control list and in the second access control list [column 7,lines 35-56];

identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list and in the second access control list [column 7,lines 35-56]; and

identifying a communication protocol for communication packets specified by each of the entries in the first access control list and in the second access control list [column 7,lines 35-56].

As to claim 25, Freed et al discloses a computer system for comparing access control lists to configure a security policy on a network, the computer system comprising:

means for identifying first sub-entries in a first access control list [column 5, lines 18-29];

means for identifying second sub-entries in a second access control list [column 5, lines 60-64];

means for programmatically determining whether a first access control list is functionally equivalent to a second access control list in order to configure the security policy on the network by determining whether each first sub-entry is equivalent to at least one of the second sub-entries [column 5, lines 38-59]; and

means for determining that the first access control list is functionally equivalent to the second access control list only when each of the first sub-entries is equivalent to at least one of the second sub-entries [column 6, lines 11-54];

wherein the means for programmatically determining whether the first access control list is equivalent to the second access control list comprise:

means for identifying a dimensional range for each policy action specified in the first access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the first access control list for that policy action [column 6, lines 11-54],

means for identifying a dimensional range for each polite action specified in the second access control list, the dimensional range of each policy action characterizing communication packets specified by entries in

the second access control list for that policy action [column 7,lines 35-56];
and

means for determining whether the dimensional range identified for each policy action in the first access control list is equivalent to the dimensional range identified for each policy action in the second access control list [column 7,lines 35-56];

wherein the means for identifying the dimensional range for each policy action specified in the first access control list and the means for identifying the dimensional range for each policy action specified in the second access control list comprises at least one means from a set of means comprising:

means for identifying a source Internet Protocol (IP) address range and a destination IP address range for communication packets specified by each of the entries in the first access control list and in the second access control list [column 7,lines 35-56];

means for identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list and in the second access control list [column 7,lines 35-56]; and

means for identifying a communication protocol for communication packets specified by each of the entries in the first

access control list and in the second access control list [column 7, lines 35-56].

As to claim 26, Freed et al discloses a policy server communicatively coupled to security devices in a network to configure a security policy on a network, the policy server comprising:

a processor [column 3 line 65 to column 4 line 27];

a network interface that communicatively couples the processor to the network to receive flows of packets therefrom [column 3 line 65 to column 4 line 27];

a memory [column 3 line 65 to column 4 line 27]; and

sequences of instructions in the memory which, when executed by the processor, cause the processor to carry out the steps of:

identifying first sub-entries in a first access control list [column 5, lines 18-29];

identifying second sub-entries in a second access control list [column 5, lines 60-64];

programmatically determining whether a first access control list is functionally equivalent to a second access control list in order to configure the security policy on the network by determining whether each first sub-entry is equivalent to at least one of the second subentries [column 5, lines 38-59]; and

determining that the first access control is functionally equivalent to the second access control list only when each of the first sub-entries is equivalent to at least one of the second sub-entries [column 7,lines 35-56];

wherein programmatically determining whether the first access control list is equivalent to the second access control list comprises:

identifying a dimensional range for each policy action specified in the first access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the first access control list for that policy action [column 7,lines 35-56];

identifying a dimensional range for each policy action specified in the second access control list, the dimensional range of each policy action characterizing communication packets specified by entries in the second access control list for that policy action [column 7,lines 35-56]; and

determining whether the dimensional range identified for each policy action in the first access control list is equivalent to the dimensional rangy identified for each policy action in the second access control list [column 7,lines 35-56];

wherein identifying the dimensional range for each policy action specified in the first access control list and in the second

access control list comprises at least one step from a set of steps comprising:

identifying a source Internet Protocol (IP) address range and a destination IP address range for communication packets specified by each of the entries in the first access control list and in the second access control list [column 7, lines 35-56];

identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list and in the second access control list [column 7, lines 35-56]; and

identifying a communication protocol for communication packets specified by each of the entries in the first access control list and in the second access control list [column 7, lines 35-56].

As to claim 27, Freed et al discloses a memory to store a plurality of access control lists, including the first access control list and the second access control list, and wherein the processor is configured to configure each security device on the network with at least one of the plurality of access control lists [column 4, lines 28-45].

As to claim 29, Freed et al discloses that the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be

Art Unit: 2131

affected by the policy action, and wherein the means for programmatically determining whether a first access control list is equivalent to the second access control list comprise:

means for determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the second access control list that specify the policy action of the entry in the first access control list [column 6 line 59 to column 7 line 34].

As to claim 30, Freed et al discloses that the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein the means for programmatically determining whether a first access control list is equivalent to the second access control list comprise:

means for determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the second access control list that specify the policy action of the entry in the first access control list [column 6 line 59 to column 7 line 34]; and

means for determining whether each entry in the second access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the first access control list that specify the same policy action [column 6 line 59 to column 7 line 34].

As to claim 31, Freed et al discloses that the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein programmatically determining whether a first access control list is equivalent to the second access control list comprises:

determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the second access control list that specify the policy action of the entry in the first access control list [column 6 line 59 to column 7 line 34].

As to claim 32, Freed et al discloses that the first access control list and the second access control list each specify a plurality of entries, and each entry identifies a dimensional range for a policy action, the dimensional range characterizing communication packets that are to be affected by the policy action, and wherein programmatically determining whether a first access control list is equivalent to the second access control list comprises:

determining whether each entry in the first access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the second access control list that specify the policy action of the entry in the first access control list [column 6 line 59 to column 7 line 34]; and

determining whether each entry in the second access control list has a dimensional range that is either equivalent to or contained by the dimensional range of entries in the first access control list that specify the same policy action [column 6 line 59 to column 7 line 34].


Art Unit: 2131

Conclusion


8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy 
May 6, 2006

CHRISTOPHER REVAH
PRIMARY EXAMINER

 5/9/06